Lecture 18

In this lecture, we'll prove various properties of isomorphisms and homomorphisms. We'll also study about automorphisms of a group.

Proposition 1 Let $\varphi : G \to \overline{G}$ be an isomorphism. Then the following hold :-

1) $\varphi(e) = \bar{e}$, $\bar{e}$ is the identity of $\overline{G}$.
2) For $a \in G$, $\varphi(a^{-1}) = [\varphi(a)]^{-1}$, i.e., φ takes inverse of an element to the inverse of the image.
3) $\forall\, n \in \mathbb{Z}$, $a \in G$, $\varphi(a^n) = [\varphi(a)]^n$.
4) G is abelian $\Longleftrightarrow$ $\varphi(G) = \overline{G}$ is abelian.
5) G is cyclic $\Longleftrightarrow$ $\overline{G}$ is cyclic. Moreover, if $G = \langle a \rangle$, then $\overline{G} = \langle \varphi(a) \rangle$.

6) For $a \in G$, $\text{ord}(a) = \text{ord}(\varphi(a))$.

7) $\varphi^{-1} : \overline{G} \longrightarrow G$ is also an isomorphism.

8) For a fixed integer k and $a \in G$, the # of solutions to the equation $x^k = a$ = # of solutions to the equation $x^k = \varphi(a)$ in $\overline{G}$.

9) If $K \leq G$ then $\varphi(K) = \{\varphi(k) \mid k \in G\} \leq \overline{G}$.

<u>Proof</u>

1) Since $\varphi : G \to \overline{G}$ is an isomorphism,

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \quad \text{—— } 1$$

Also, since $\varphi(e) \in \overline{G}$ and $\overline{e}$ is the identity of $\overline{G}$ so

$$\varphi(e) = \varphi(e) \cdot \overline{e} \quad \text{— } 2$$

from 1 and 2, we get

$\varphi(e) \cdot \overline{e} = \varphi(e) \cdot \varphi(e)$, so by cancellation law,

$$\varphi(e) = \overline{e}.$$

2) For $a \in G$,

$$aa^{-1} = e \Rightarrow \varphi(aa^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = \varphi(e) = \bar{e}$$

$$\Rightarrow [\varphi(a)]^{-1} = \varphi(a^{-1})$$

3) Just follows from the definition of an isomorph-
-ism.

4) We'll just prove one direction as the other direction follows from 7).

Let G be abelian. Pick $x, y \in \bar{G}$. Since φ is onto, $\exists$ $a, b \in G$ s.t. $\varphi(a) = x$

$$\varphi(b) = y$$

So $$x \cdot y = \varphi(a) \cdot \varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b) \cdot \varphi(a)$$

$$= y \cdot x$$

5) Again we'll just prove one direction. It's enough to show that $\varphi(a)$ is a generator of $\bar{G}$.

Let $x \in \bar{G}$. Since φ is onto, $\exists$ $b \in G$ s.t.

$\varphi(b) = x$. But $G = \langle a \rangle \Rightarrow b = a^n, n \in \mathbb{Z}$.

So, $\varphi(a^n) = x$. From 3), we get

$\varphi(a^n) = [\varphi(a)]^n = x \Rightarrow \bar{G} = \langle \varphi(a) \rangle$.

6) Let $a \in G$ and $\mathrm{ord}(a) = n$. Then $a^n = e$.

We know then, $\bar{e} = \varphi(e) = \varphi(a^n) = [\varphi(a)]^n$

so, $\mathrm{ord}(\varphi(a)) \mid n$.

If $\mathrm{ord}(\varphi(a)) = k \Rightarrow \varphi(a)^k = \bar{e}$

$\Rightarrow \varphi(a^k) = \bar{e} = \varphi(e)$

Since, φ is one-one $\Rightarrow a^k = e \Rightarrow n \mid k$

so $n \mid k$ and $k \mid n \Rightarrow k = n$ and hence $\mathrm{ord}(\varphi(a)) = n$.

7). φ is a bijection, so $\varphi^{-1} : \bar{G} \to G$ is a bijec-
-tion. Let $x, y \in \bar{G}$. Then $\exists$ $a, b \in G$ s.t.
$\varphi(a) = x$ and $\varphi(b) = y$.

So, $\varphi^{-1}(x \cdot y) = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(ab))$

$$= ab = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$$

So, φ^{-1} is a homomorphism as well.

8) If $b \in G$ is a solution of $x^k = a$, i.e., $b^k = a$ then $\varphi(b)$ is a solution of $x^k = \varphi(a)$.

So # of solutions in G $\leq$ # of solutions in $\bar{G}$

But we can do the same thing with $\varphi^{-1} : \bar{G} \to G$

so # of solutions in $\bar{G}$ $\leq$ # of solutions in G

and hence the result.

9) Left as an exercise.

$\boxed{\checkmark}$

So with the help of the above properties, we can tell when two groups are not isomorphic.

e.g. Consider $U(10)$ and $U(12)$.

$U(10) = \{1, 3, 7, 9\}$

$U(12) = \{1, 5, 7, 11\}$

We saw that $U(10) \cong \mathbb{Z}_4$. Is $U(10) \cong U(12)$?

Note that it's not hard to come up w/ a bijection between $U(10)$ and $U(12)$. So all we need to check is that whether there is a homomorphism b/w them.

Note that $U(10) = \langle 3 \rangle$.

However, the orders of elements in $U(12)$ are

1 — order 1
5 — order 2
7 — order 2
11 — order 2

So $U(12)$ can't be cyclic and so from 5) can't be isomorphic to $U(10)$.

e.g. Is $(\mathbb{C}^*, \times) \cong (\mathbb{R}^*, \times)$

where $\mathbb{C}^* = \{ x \in \mathbb{C} \mid x \neq 0 \}$

$\mathbb{R}^* = \{ x \in \mathbb{R} \mid x \neq 0 \}$

Note that if $\varphi : \mathbb{C}^* \longrightarrow \mathbb{R}^*$ is an isomorphism, then $\varphi(1) = 1$ as 1 is the identity in both $\mathbb{C}^*$ and $\mathbb{R}^*$.

Let's look at the equation $x^4 = 1$. In $\mathbb{C}^*$ it has 4 solutions : $1, -1, i, -i$

In $\mathbb{R}^*$, the equation $x^4 = \varphi(1) = 1$ has only two solutions : $1, -1$

So from 8) $(\mathbb{C}^*, \times) \ncong (\mathbb{R}^*, \times)$. [not isomorphic]

Automorphisms

There are some isomorphisms which are very important and hence must be discussed separately.

Defⁿ :- Let G be a group. An isomorphism of G onto itself is called an automorphism.

e.g. 1) The identity map $I : G \to G$ is clearly an automorphism.

2) Consider $\phi : (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$ given by

$$\phi(a+ib) = a - ib$$

This is an automorphism.

Suppose G is a group. Is there any other autom-orphism of G apart from the identity?

Defⁿ (Inner automorphism induced by a)

Let G be a group and $a \in G$. The map $\varphi_a : G \to G$ given by $\varphi_a(g) = aga^{-1}$ is an automorphism of G called the inner automorphism of G induced by a.

Check that φ_a is a bijection.

To see that φ_a is a homomorphism :- Let $g, h \in G$, then

$$\varphi_a(g \cdot h) = agha^{-1} = aga^{-1}aha^{-1}$$
$$= \varphi_a(g) \cdot \varphi_a(h)$$

Thus there are many automorphism of a group.

Note that :- $\varphi_e(g) = ege^{-1} = g$

So, $\varphi_e = I$. Can $\varphi_a = I$ for any $a \in G$, $a \neq e$? We'll see the answer to this question after the First Isomorphism Theorem.

<u>Theorem</u> 1 Let $Aut(G) = \{ \varphi : G \to G \mid \varphi \text{ is an isomorphism} \}$ be the set of automorphism of G. Then $Aut(G)$ is a group with the operation "$\circ$" which is

composition of functions.

If $\text{Inn}(G)$ denote the set of inner automorphisms of G, then $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$, i.e. $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

<u>Proof</u>:- The fact that $\text{Aut}(G)$ is a group and $\text{Inn}(G) \leq \text{Aut}(G)$ are left as exercises. To prove $\text{Inn}(G) \triangleleft \text{Aut}(G)$, we use the normal subgroup test. Let $\varphi \in \text{Aut}(G)$ and $f_a \in \text{Inn}(G)$ for some $a \in G$.

<u>Claim</u>:- $\varphi f_a \varphi^{-1} \in \text{Inn}(G)$.

So we want to prove that $\exists\, b \in G$ s.t. $\varphi f_a \varphi^{-1} = f_b$ for that b. Let $g \in G$. Then

$$\varphi f_a \varphi^{-1}(g) = \varphi(f_a(\varphi^{-1}(g)))$$

$$= \varphi(a^{-1}\varphi^{-1}(g)a) \quad (\text{by the def}^n \text{ of } f_a)$$

$$= \varphi(a^{-1}).\varphi\varphi^{-1}(g).\varphi(a)$$

$$= \varphi(a)^{-1} g \cdot \varphi(a)$$

So from this we see that if we choose

$b = \varphi(a)$, then

$$\varphi f_a \varphi^{-1} = b^{-1} g\, b = f_b \in \mathrm{Inn}(G).$$

Hence, $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

In the next lecture we'll compute $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ for specific groups and then proceed to under homomorphisms.

o ———— x ———— x ———— o